SISTEMA INTEGRAL DE COMUNICACIÓN SEGURA BASADO EN POWERLINE

Fernando Méndez Rebollo

fernando_mendez@ieee.org

Universidad de Alcalá – Escuela Politécnica, Campus Universitario, Ctra. Madrid-Barcelona Km. 33.600 28806 Alcalá de Henares (Madrid), España.

ABSTRACT

En este artículo se presenta un sistema digital de comunicación basado en subsistemas Powerline y Ethernet. El fin perseguido es proveer de un canal de comunicación segura a cualquier aparato conectado a la red eléctrica. Sus principales ventajas son fiabilidad, escalabilidad, facilidad de instalación y bajo coste. El hardware de transmisión sobre red eléctrica ha sido diseñado para cumplir con los estándares CENELEC y debido a su precio y tamaño, puede ser incorporado a casi cualquier dispositivo eléctrico. La seguridad está garantizada mediante el uso de SSL en el enlace Ethernet y SSL o TEA-Block sobre el enlace Powerline. Se ha prestado especial atención a la gestión del sistema, siendo éste capaz de detectar nuevos elementos en la red y configurarlos automáticamente.

1. INTRODUCCIÓN

La solución que se presenta a continuación pretende abordar la implementación de un sistema de comunicación segura extendida a través de la red eléctrica doméstica de 125 ó 220V y 50 ó 60Hz. Las principales características que se han impuesto como requisitos del sistema son: facilidad de integración en un entorno doméstico o laboral, escalabilidad, inmunidad ante ataques contra la seguridad del sistema y bajo coste.

Aunque las aplicaciones para este tipo de red de comunicación son innumerables en el campo de la domótica, este artículo se centra en la implementación de un sistema antirrobo para todo tipo de aparatos eléctricos conectados a la red eléctrica. Este concepto es objeto de la patente en trámite número: P200300038, presentada por el autor en Enero de 2003.

El sistema aquí presentado pretende cumplir con las restricciones que una aplicación de este tipo impone al diseño. La idea general para abordar el problema es utilizar la red eléctrica como medio de transmisión, por el que se mantendrá una comunicación constante con los aparatos que pudieran ser sustraídos. Si un aparato intenta ser robado, necesariamente ha de ser desconectado de la red eléctrica, con lo que se pierde la comunicación y se detecta el hurto. Un equipo maestro debería ser el encargado de manejar todas las comunicaciones y de iniciar la alarma en caso de hurto, pero ya que la distancia de transmisión sobre red eléctrica es limitada, serán necesarios varios maestros. Para poder controlar todo el conjunto de forma centralizada, se ha optado por conectar todos los equipos maestros a la red de área local presente en el edificio en el que se quiere instalar el sistema. De esta forma, se puede situar en cualquier parte de la red una consola central de monitorización. Esta consola tendrá un control total y a través de ella se informará de los posibles hurtos.

Se intentará dar solución a todos los problemas que históricamente han tenido este tipo de sistemas distribuidos [1]. Existen varias ventajas en la utilización de la red eléctrica para la comunicación de información en un sistema de seguridad, entre las que destacan:

1) La infraestructura de red ya existe.
2) La red eléctrica se extiende a todos los puntos de un edificio.
3) Los equipos a proteger se encuentran constantemente conectados al medio.
4) Es fácil implementar un canal de bajo ancho de banda sobre red eléctrica.
5) Es imposible saber a priori si un equipo está o no siendo monitorizado.

Como desventajas principales de este medio de comunicación se tiene:

1) El ancho de banda se contrapone a la distancia máxima de comunicación en implementaciones de bajo coste.

2) La distancia máxima de transmisión está además limitada por factores como la atenuación del canal y la topología de la red.

3) El ruido introducido en la red eléctrica por otros aparatos a ella conectados, puede disminuir las prestaciones del conjunto.

El hecho de tener un ancho de banda limitado, no es crítico en un sistema que sólo pretenda dotar de protección antirrobo a los equipos eléctricos, ya que la información enviada es mínima. El problema más grave es, por tanto, la distancia máxima de transmisión. Este problema es solventado mediante el uso adicional de una red de área local. Para explotar de forma lógica ambas redes, se utilizan dos tipos de dispositivos en concordancia con lo ya expuesto:

1) Esclavos: Dispositivos que serán incorporados a los equipos eléctricos que desean ser protegidos contra robo. Este dispositivo sólo dispone de comunicación a través de la red eléctrica y por tanto no podrá comunicarse a grandes distancias.

2) Maestros: Dispositivos capaces de conectarse tanto a la red eléctrica como a la red de área local y que harán de nexo entre ambas redes. Así, un maestro da la posibilidad de comunicación a través de la red de área local a todos aquellos esclavos que se encuentren a una distancia inferior a 200 metros.

La figura 1 proporciona una visión general de la arquitectura.

En las siguientes secciones, se abordará primeramente el funcionamiento general del sistema, tras lo cual se describirán los distintos medios de transmisión utilizados. A continuación se expondrá el hardware empleado y por último se describirán los protocolos y sistemas de seguridad aplicados.

2.FUNCIONAMIENTO DEL SISTEMA

Para cumplir con las especificaciones, se ha optado por incluir en la fuente alimentación de cada equipo eléctrico que quiere ser protegido contra robo, un dispositivo esclavo capaz de comunicarse a través de la conexión a la red eléctrica del propio aparato. Esto posibilita la instalación del sistema sin variación de las infraestructuras del edificio. Así, una vez que los equipos están dotados de esta vía de comunicación, pueden ser interrogados constantemente para garantizar su presencia, de tal forma que un equipo que sea desconectado del enchufe será incapaz de responder a tales requerimientos.

Como ya se ha dicho anteriormente, las comunicaciones a través de la red eléctrica tienen notables limitaciones de distancia, por lo que será necesario que el dispositivo encargado de realizar el control de los esclavos sea un dispositivo con conexión a la red de área local. Por ejemplo, en un edificio de oficinas, donde se requiere tener un control centralizado de todos los ordenadores alojados en las distintas plantas, será necesario disponer de varios maestros.

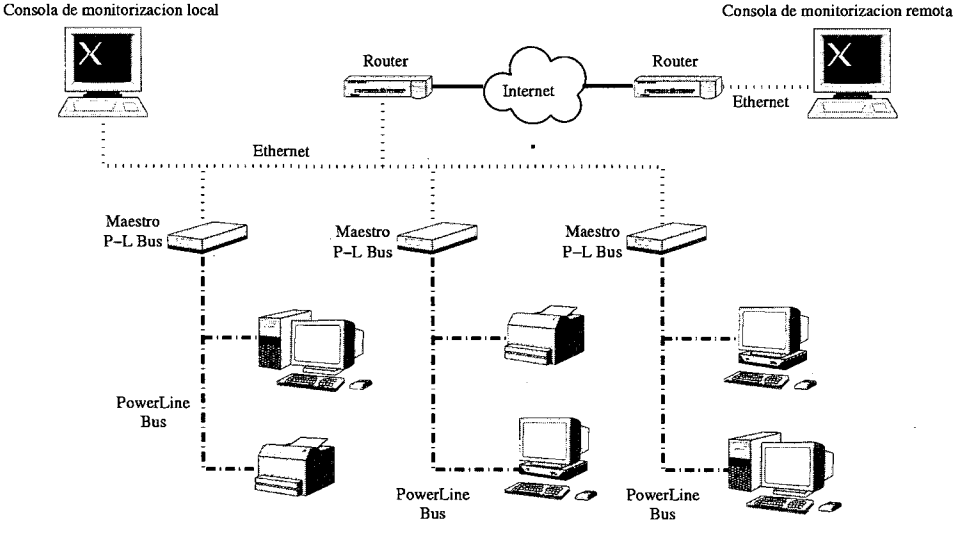

Figura 1. Implementación del sistema

Este tipo de red, representa la realidad de las comunicaciones informáticas de la inmensa mayoría de entornos laborales, por lo cual será accesible desde casi cualquier parte del edificio. Así pues, existirá una consola central encarga de realizar en última instancia la monitorización de los aparatos que se quieren proteger. Para ello, preguntará a los distintos maestros dentro del edificio sobre la presencia o ausencia de los equipos que residen bajo su control. Los maestros a su vez estarán encargados de mantener la comunicación con todos los esclavos bajo su control y poner esta información a disposición de la consola central. De esta forma si un aparato es sustraído, el maestro al que estaba conectado registra su ausencia y comunica tal información a la consola central. De semejante manera, si un maestro es eliminado, la consola central perderá la comunicación con él e informará de tal suceso.

3.DESCRIPCIÓN DE LOS MEDIOS DE TRANSMISIÓN

3.1.Red eléctrica doméstica

La red eléctrica doméstica posee unas características bastante inusuales bajo el punto de vista de los medios tradicionales de comunicación [2]. Uno de los puntos más conflictivos a la hora de caracterizar este medio, es el hecho de que no cumple dos de las condiciones necesarias para poder aplicar el teorema de superposición de señales. Así, en muchas ocasiones, la red eléctrica no cumple condiciones de linealidad ni de invarianza en el tiempo. Otro problema que se presenta en la utilización de este medio de transmisión, es el ruido de múltiples tipos que es inyectado en la red eléctrica por los aparatos a ella conectados. En la figura 2 se representan algunas de las fuentes de ruido más comunes en entornos domésticos.

El ruido producido por estos aparatos puede clasificarse de la siguiente manera:

1) Ruido impulsivo de baja frecuencia: Tiene frecuencia doble de la corriente alterna de la red. Es generado principalmente por aparatos que utilicen triacs, como por ejemplo reguladores de luz.

2) Ruido tonal: Es generado principalmente por las fuentes de alimentación conmutadas. Su frecuencia fundamental puede estar en el rango desde 20KHz hasta 1MHz.

3) Ruido impulsivo de alta frecuencia: Es producido por motores de corriente alterna conectados a la red. Su frecuencia es de varios kilohercios.

En nuestro análisis, las premisas de utilización pasan por utilizar la red eléctrica para realizar comunicaciones a distancias alrededor de 200 metros con frecuencias en torno a 135KHz. En este caso, la longitud de cable es inferior a 1/8 de la longitud de onda efectiva de la señal. Esto permite asumir que la degradación del canal debida a efectos de onda estacionaria será despreciable. Esta banda se encuentra lo suficientemente alejada de la señal de potencia a 50Hz, lo que hace posible separar la potencia eléctrica de la señal que porta la información. Dicha banda de frecuencias es objeto del estándar CENELEC EN 50065-1 que regula la utilización de la banda entre 3KHz y 148,5KHz en instalaciones eléctricas.

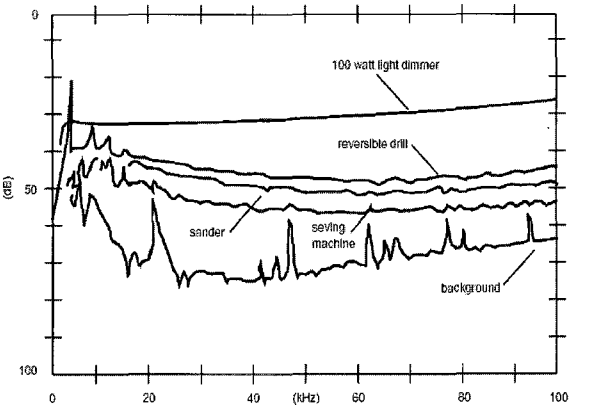

Figura. 2. Diagrama espectral de algunas fuentes comunes de ruido en powerline

Siguiendo con una filosofía de bajo coste se ha optado por la utilización de un modem FSK con 2 portadoras a 133,05KHz y 131,85KHz respectivamente [4]. El medio restringe las posibilidades a un modo half duplex con un régimen binario de 4800bps. A las citadas distancias también son notables los efectos por atenuación. La figura 3 muestra algunas atenuaciones típicas para distintos caminos de propagación encuadrados en un entorno doméstico. Se han podido realizar transmisiones exitosas a distancias de 200 metros, observándose atenuaciones medias en amplitud de 25dB. Es esta limitación la que obligará a asociar a los equipos esclavos en grupos, marcados por su cercanía entre sí.

Éstos a su vez, deben comunicarse con una consola central de supervisión. Para realizar tal comunicación, los maestros utilizan la red de área local. En la implementación actual, los maestros disponen de interfaz para conectarse a redes Ethernet.

Cada uno de estos grupos se caracteriza porque los esclavos que a él pertenecen, comparten el mismo bus de comunicación a través de la red eléctrica. Se denominará a cada uno de estos buses PL-Bus (PowerLine Bus).

Cada PL-Bus será monitorizado por un equipo maestro, que se encargará además de relacionar a todos los equipos esclavos con la consola central de monitorización. Ésta es la razón de la adopción del segundo medio de transmisión, la red de área local Ethernet, que será la encargada de comunicar a todos los maestros de PL-Bus con la consola central de monitorización.

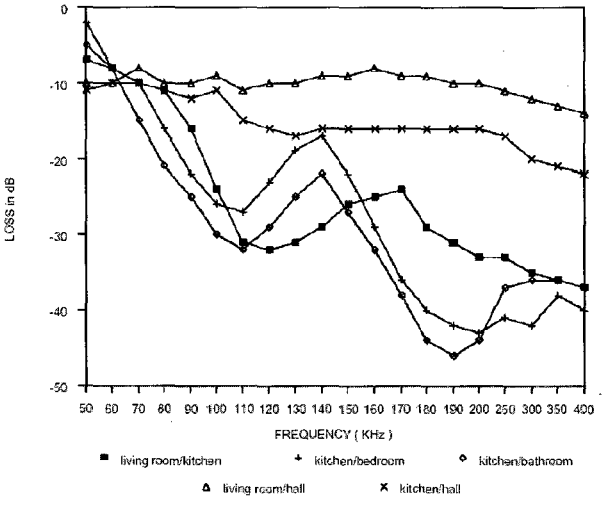

Figura 3. Atenuación de la red eléctrica por distintos caminos (Por Daniel Chaffanjon)

3.2.Red de área local Ethernet

Este tipo de redes son actualmente una constante en cualquier entorno empresarial. El caso más extendido en entornos laborales es aquel en el que los equipos de dicha red de área local tienen acceso a Internet a través de un gateway.

Este caso proporciona la posibilidad de instalar la consola de monitorización central en un punto remoto, permitiéndose así el control a distancia e incluso la posibilidad de controlar de forma centralizada varios edificios. La estructura de este esquema puede observarse en la figura 1.

Una de las ventajas de las tecnologías de Internet es la madurez de los métodos de protección de datos, que serán discutidos más adelante.

4.HARDWARE UTILIZADO

4.1.Esclavos

Cada esclavo dispone de una fuente de alimentación conmutada independiente de la alimentación del aparato al que se adhiere. Esto permite que el sistema de protección funcione incluso cuando el aparato no esté en funcionamiento. El sistema de comunicación por el que acceden al PL-Bus consta de una interfaz de aislamiento, que discrimina la banda de comunicaciones, una sección de amplificación para la señal de salida y un modem FSK.

El modem está dotado de un detector de portadora independiente del correlador, que es imprescindible para la detección de errores irrecuperables en el protocolo de comunicaciones. Dispone además de la posibilidad de sensar la señal de entrada tras un pequeño filtrado que facilita la medida. El módulo de control del esclavo es un microcontrolador de 8 bits. Éste es el encargado de implementar la máquina de estados que gobierna el sistema y de realizar la encriptación y desencriptación de la información. Este microcontrolador, gracias a un ADC es capaz de realizar medidas de amplitud de la señal de entrada al modem. Esta característica permite la ejecución de un algoritmo de autogestión, por el cual, esclavos y maestros son capaces de agruparse automáticamente basando esta asociación en el sensado de la amplitud de las portadoras de cada equipo. Así cada esclavo escoge al maestro al que recibe con mayor amplitud. Este algoritmo será discutido más adelante. Las medidas de amplitud, son además útiles para caracterizar el medio y poder planificar la inserción de maestros de PL-Bus en zonas donde la señal está muy debilitada.

4.2. Maestros de PL-Bus

Aunque el modelo en el que se trabaja actualmente implementa los equipos maestros mediante el mismo hardware que los esclavos y mediante una conexión RS-232 a un PC, se prevé el diseño de hardware específico para éstos.

La propuesta más interesante la compone el uso un microprocesador embebido, lo que conferiría a los maestros las altas prestaciones de cálculo necesarias para resolver los esquemas de autenticación necesarios en las comunicaciones sobre Internet.

La utilización de un microprocesador embebido, permite además la inclusión de un sistema operativo, lo que facilita notablemente la tarea de desarrollar software para los dispositivos maestros. Actualmente existen en el mercado varias alternativas, siendo las más estudiadas aquellas que ofrecen una solución basada en un único chip que implementa procesador, sistema de almacenamiento e interfaz Ethernet. En cuanto al sistema operativo, se ha escogido GNU/Linux como plataforma de desarrollo. Éste ofrece implementación completa de todos los protocolos de red, librerías de autenticación y aplicaciones en código abierto, permitiendo la adaptación a las necesidades específicas que se requieran. GNU/Linux dispone además de herramientas de desarrollo de gran calidad, lo que facilitará la generación del software necesario.

4.3.Consola central de monitorización

Esta consola es propiamente un ordenador personal. Esto mejora la capacidad para interactuar con el usuario y permite implementar de forma cómoda todos los algoritmos de encriptación necesarios y la representación gráfica. Esta consola podrá ser local o remota, ya que la señalización de control puede enviarse de forma segura a través de Internet gracias a la utilización de SSL en las comunicaciones con los maestros.

5.PROTOCOLOS DE COMUNICACIÓN

5.1.Comunicaciones en PL-Bus

Las comunicaciones utilizadas sobre el PL-Bus se basan en una trama de comunicaciones que engloba el nivel de enlace y red en una única trama semejante a HDLC (High Level Data Link Control). En la figura 4 puede observarse la estructura de campos de dicha trama.

La trama comienza con una secuencia de entrenamiento, que produce la puesta en marcha de los correladores en los receptores así como de los detectores de portadora.

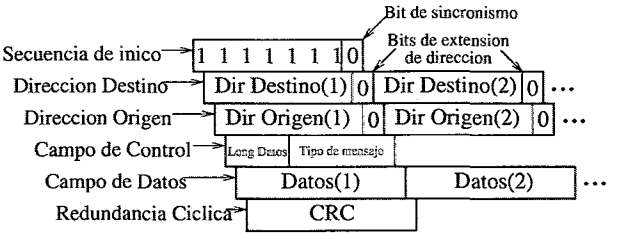

Figura. 4. Trama de Pl-Bus.

Esta secuencia termina con un bit a nivel bajo que permite la sincronización de la trama en el flaco de bajada. Obsérvese que el detector de portadora es imprescindible para discernir las auténticas secuencias de entrenamiento, ya que éstas sólo aparecen cuando el detector de portadora indica ausencia de portadora.

La dirección es ampliable y crece en bloques de 7 bits, lo que proporciona una escalabilidad sólo limitada por los retardos de transmisión. El campo de control reserva 3 bits para indicar la longitud del campo de datos, de tal forma que se pueden seleccionar tamaños de campo de datos de entre 0 y 64 bytes. Así, la relación que indica el tamaño del campo de datos es:

$$datos = 2^{long-1}$$

salvo el caso del cero, que se computa directamente como la anulación del campo de datos. Los otros 5 bits del campo de control, indican el tipo de mensaje.

Entre estos tipos de mensajes se establecen primitivas para ceder el bus a una entidad superior con capacidad de autenticación por medio de la autoridad certificadora implementada en la consola central. Otras primitivas implementadas son el ping simple, o las primitivas que permiten la aceptación en el bus de un nuevo esclavo que será verificado por la autoridad certificadora.

El proceso de aceptación de un nuevo esclavo es completamente automático, no requiriéndose ningún tipo de conocimiento sobre la organización zonal de los PL-Bus. La última implementación realizada del sistema pretende además el autonegociado de agrupación de maestros y esclavos de forma automática basándose en la amplitud de las portadoras recibidas, para lo que se ha desarrollado un protocolo más. En la implementación actual, los datos contenidos en el paquete se transmiten encriptados.

El algoritmo de encriptación utilizado es TEA-Block [5], ya que la potencia de cálculo requerida por éste es asumible para un microcontrolador de 8 bits.

Todos los esclavos y maestros poseen una clave preprogramada en memoria, lo que evita tener que distribuir la primera clave para iniciar la comunicación.

Así, como se aprecia en la figura 5, esta clave es adecuada para cifrar un primer mensaje de intercambio de clave de sesión. Esta clave de sesión, distribuida en tiempo de ejecución es diferente para cada esclavo y tiene un tiempo de vida que depende del número de esclavos en el bus. La figura 5 muestra el proceso de intercambio de una nueva clave de sesión.

Se realizará una futura mejora de este sistema de encriptación, haciendo uso de una implementación de Serpent [6], una propuesta para AES (Advanced Encryption Standard). Serpent admite implementaciones que no requieren de elevadas capacidades de procesado, lo que hace factible su utilización con microcontroladores de 8 bits, a la vez que supera la protección contra ataques de fuerza bruta que otros métodos como triple-DES ofrecen. Otra posibilidad dependiente del desarrollo de precios de los ya citados procesadores embebidos, es la utilización de éstos tanto en dispositivos maestros como en esclavos, lo que mejoraría la seguridad y facilitaría el desarrollo del sistema debido a la unificación de las arquitecturas hardware. Una implementación de este tipo permitiría la utilización de SSL también en las comunicaciones a través de Powerline.

Para minimizar el ancho de banda consumido por las peticiones de respuesta del maestro, éstas son eliminadas en su mayoría. En lugar de solicitar a cada esclavo una respuesta cifrada con la clave de sesión, se realiza una asignación de turno por token.

El maestro indicará un número aleatorio que cada esclavo deberá responder encriptando con la clave de sesión en su turno de token. El maestro indica a cada esclavo cual es su turno enviándole la dirección del esclavo inmediatamente anterior a él en el bus.

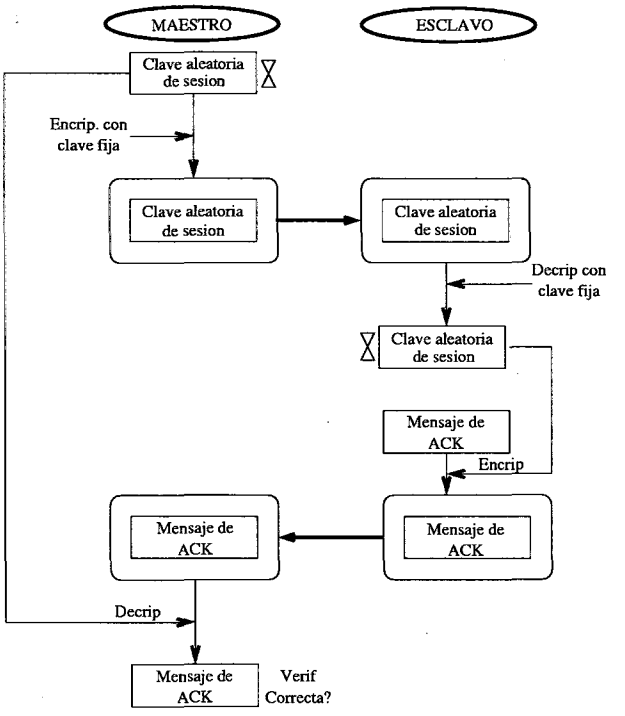

Figura. 5. Intercambio de clave de sesión en PL-Bus.

Así cada esclavo responde en su turno de token sin intervención del maestro, que sólo tiene como misión la verificación de los mensajes. Sólo se producen comunicaciones directas entre un esclavo y su maestro en situaciones de cambio de posición en el bus, intercambio de nueva clave de sesión o errores de autenticación. El maestro puede cambiar el orden de los esclavos después de un tiempo aleatoriamente generado. Todos estos procesos, dificultan enormemente la suplantación de un esclavo, elevando así el nivel de seguridad.

Como sistema de detección de errores, el sistema utiliza un campo de CRC de 1 byte. Para la generación de esta redundancia se utiliza el polinomio $x^8 + x^2 + x + 1$

Esta redundancia permite detectar cualquier error en 1 bit, cualquier número impar de bits erróneos y cualquier salva de error de menos de 8 bits [7].

5.2. Autonegociado y autoconfiguración del sistema

La última implementación del sistema pretende dotar a éste de funcionalidad adicional que permita una administración del sistema más sencilla. Uno de los problemas más graves en PL-Bus es la situación dentro de la red eléctrica de maestros y esclavos y qué maestro es asignado a cada esclavo.

El pad marcado como RAI indica la entrada de la señal de la red eléctrica tras pasar la etapa de adaptación al medio.

Obsérvese que en el punto marcado como RxFO se obtiene la señal filtrada antes de ser amplificada. La señal extraída en este punto será sensada, de tal forma que se puede obtener la amplitud.

Este valor será indicativo de la potencia con la que se está recibiendo una fuente. Este proceso de sensado se realizará para cada una de las portadoras recibidas de los distintos maestros cercanos.

El conjunto se comporta de la siguiente manera:

Cada 20 segundos, los maestros inician un periodo de aceptación de nuevos esclavos. Estos periodos están sincronizados entre los maestros a través de la Ethernet, de tal forma que no choquen en sus emisiones por la red eléctrica. El proceso

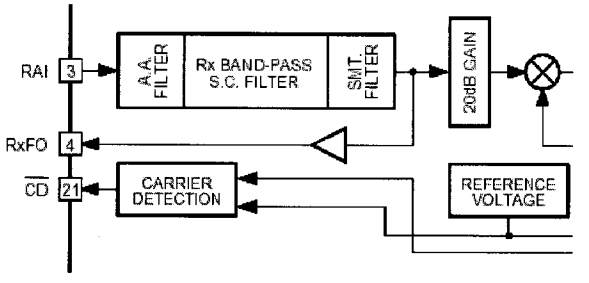

Figura. 6. Detalle de la estructura interna del modem utilizado.

consta de la emisión consecutiva de secuencias de entrenamiento por parte de cada maestro.

El esclavo interesado en registrarse en el sistema, recibirá todas las secuencias y decidirá cual tiene mejor nivel de señal. Tras esto, existe un periodo de contienda, en el que todos los esclavos interesados en registrarse intentarán hacerlo.

Si existe choque, los maestros lo sabrán, pues detectarán las portadoras, pero la trama recibida estará corrupta (CRC no válido). En tal caso, los maestros no responden y los esclavos darán por hecho que han chocado, esperando un tiempo aleatorio antes de reintentarlo.

El choque sólo sucede si la emisión de al menos 2 esclavos comienza en el mismo instante, puesto que si uno de ellos empieza a transmitir, el resto de esclavos detectan su portadora y no intentan emitir.

Las claves de todos los procesos concernientes a la detección de choques, se basan en la utilización del detector de portadora y la verificación del CRC de las tramas.

5.3. Comunicaciones en Ethernet

Ya que los mensajes se transmitirán por la misma red corporativa, éste es el punto más evidente para un ataque de seguridad por suplantación. Además, si la consola de monitorización es remota, los mensajes entre maestros y consola serán enrutados vía Internet, lo que provoca un nuevo problema de seguridad.

Para evitar las agresiones contra esta parte del sistema de seguridad, se ha optado por la implantación de SSL (Secure Socket Layer) para proporcionar el nivel de seguridad necesario en las transacciones.

SSL puede ser utilizado sobre cualquier protocolo de transporte, en nuestro caso TCP/IP. SSL confiere al canal de comunicaciones privacidad, autenticidad e integridad.

SSL utiliza certificados X.509, un esquema de clave pública/clave privada y una suite de cifrado que cuenta entre otros algoritmos con Triple-DES, MD5, RSA y RC4 [8].

SSL se alza como una de las soluciones integrales más extendidas en Internet, ya que autentica al cliente y al servidor, cifra el canal y asegura la integridad de los datos.

La implementación completa de SSL está disponible como código abierto bajo licencia GNU, lo que acorta enormemente el tiempo de desarrollo. Ya que actualmente SSL es el estándar de facto para seguridad en Internet, no se entra en más detalles sobre su implementación.

6.CONCLUSIONES

Se ha presentado un sistema de comunicación segura adaptable a prácticamente cualquier equipo conectado a la red eléctrica.

Una aplicación interesante es la utilización de este desarrollo en un sistema de control antirrobo. El sistema cumple con las premisas de fiabilidad, solidez ante ataques, bajo coste y fácil integración y administración.

La seguridad ha sido una prioridad y por ello se han implementado métodos de autenticación que permiten administrar el sistema desde Internet sin temer por la seguridad del sistema.

El futuro inmediato del desarrollo pasa por la mejora de la encriptación sobre powerline, la implementación de un hardware definitivo para los equipos maestros y la verificación del funcionamiento del algoritmo de autonegociado de maestro.

REFERENCIAS

[1] RJ Anderson, SJ Bezuidenhoudt, "On the Reliability of Electronic Payment Systems", IEEE Transactions on Software Engineering v 22 no 5, May 1996.

[2] Phil Sutterlin, "A Power Line Communication Tutorial - Challenges and Technologies", Proceedings of the 1998 International Symposium on Power-line Communications and its Applications Soka University, Tokyo, March 1998.

[3] Roger M. VINES, Jel TRUSSEL, Louis J. GALE, "Noise on Residential power distribution circuits", IEEE Transactions on Electromagnetic Compatibility, Vol EMC-26, N°24, pp 161-168, November 1984.

[4] S.G. Wilson, *«Digital Modulation and Coding»*, Prentice-Hall, 1996.

[5] David Wheeler and Roger Needham, "TEA, a Tiny Encryption Algorithm", Proceedings of the K. U. Leuven Workshop on Cryptographic Algorithms. Springer-Verlag, 1995.

[6] Anderson, Ross and Eli Biham, "Serpent: A Proposal for the Advanced Encryption Standard", NIST AES Proposal, June 1998.

[7] S.B. Wicker, "Error Control Systems for Digital Communication and Storage", Prentice-Hall, 1995.

[8] John Ousterhout, "Timing attacks on implementetion of Diffie-Hellman, RSA, DSS, and other systems", Lecture Notes in Computer Science, vol.1109, Springer-Verlag, 1996.

AUTOR

Fernando Méndez Rebollo nació en León en 1980. Actualmente es becario de investigación del Departamento de Electrónica de la Universidad de Alcalá (Madrid), donde realiza el proyecto fin de carrera de la titulación de Ingeniería de Telecomunicación en el campo de la visión artificial mediante arquitecturas hardware basadas en FPGA's.

Otro campo de interés es la robótica, habiendo formado parte del primer equipo español competidor en el campeonato europeo de robótica Eurobot2002.

En el campo de la domótica, colabora en un proyecto del Departamento de Electrónica de la Universidad de Alcalá para el desarrollo de una plataforma domótica integral para la interacción de un robot móvil de ayuda a la discapacidad con un entorno doméstico automatizado, utilizando tecnología Home-Plug.